

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
4. Mai 2006 (04.05.2006)

PCT

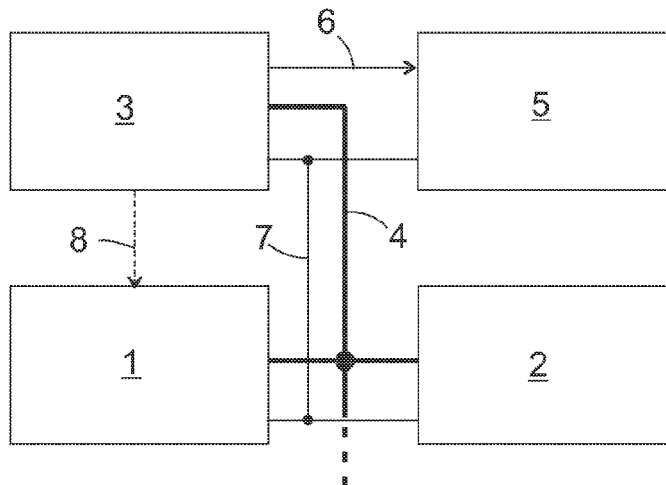
(10) Internationale Veröffentlichungsnummer
WO 2006/045807 A2

- (51) Internationale Patentklassifikation: **Nicht klassifiziert**
- (21) Internationales Aktenzeichen: PCT/EP2005/055549
- (22) Internationales Anmeldedatum:
25. Oktober 2005 (25.10.2005)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2004 051 950.1
25. Oktober 2004 (25.10.2004) DE
10 2004 051 992.7
25. Oktober 2004 (25.10.2004) DE
10 2005 045 399.6
23. September 2005 (23.09.2005) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02
20, 70442 Stuttgart (DE).
- (72) Erfinder; und
- (73) Erfinder/Anmelder (nur für US): **COLLANI, Yorck**
[DE/DE]; Lisztweg 9, 71717 Beilstein (DE). **KOTTKE,**
Thomas [DE/DE]; Leimentalstrasse 13/1, 71139 Ehningen
(DE).
- (74) Gemeinsamer Vertreter: **ROBERT BOSCH GMBH;**
Postfach 30 02 20, 70442 Stuttgart (DE).
- (81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY,
MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO,
NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK,
SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.
- (84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: DATA PROCESSING SYSTEM WITH A VARIABLE CLOCK SPEED

(54) Bezeichnung: DATENVERARBEITUNGSSYSTEM MIT VARIABLER TAKTRATE



(57) Abstract: A data processing system comprises an execution unit (1) that functions in a clocked manner, a clock generator (5) for supplying a clock signal for the execution unit (1), and a monitoring unit (3) for monitoring the proper functioning of the execution unit (1). The clock generator (5) is designed for supplying the clock signal with a controllable frequency. The monitoring unit (3) is functionally connected to the clock generator (5) in order to lower the frequency of the clock signal when it has been established that the execution unit (1) is functioning improperly.

[Fortsetzung auf der nächsten Seite]

WO 2006/045807 A2



GII, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

- *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

(57) Zusammenfassung: Ein Datenverarbeitungs System umfasst eine getaktet arbeitende Ausführungseinheit (1), einen Taktgenerator (5) zum Liefern eines Taktsignals für die Ausführungseinheit (1) und eine Überwachungseinheit (3) zum Überwachen des ordnungsgemäßen Arbeitens der Ausführungseinheit (1). Der Taktgenerator (5) ist eingerichtet, das Taktsignal mit einer steuerbaren Frequenz zu liefern. Die Überwachungseinheit ist (3) funktionsmäßig mit dem Taktgenerator (5) verbunden, um die Frequenz des Taktsignals herabzusetzen, wenn nichtordnungsgemäßes Arbeiten der Ausführungseinheit (1) festgestellt wird.

5

Datenverarbeitungssystem mit variabler TaktrateStand der Technik

10

Die vorliegende Erfindung betrifft ein Datenverarbeitungssystem mit einer getaktet arbeitenden Ausführungseinheit wie etwa einem Mikroprozessor, einem Taktgenerator zum Liefern eines Taktsignals für
15 die Ausführungseinheit und einer Überwachungseinheit zum Überwachen des ordnungsgemäßen Arbeitens der Ausführungseinheit.

Solche Überwachungseinheiten, die auch unter der
20 Bezeichnung „Watchdog“ bekannt sind, dienen herkömmlicherweise dazu, einen undefinierten Zustand bzw. Absturz der Ausführungseinheit zu erkennen und erforderlichenfalls die Ausführungseinheit zurückzusetzen, um einen definierten Betriebszustand wieder herzustellen. Ein solcher „Watchdog“ ist in der
25 Lage, unter Inkaufnahme einer zeitweiligen Betriebsunterbrechung der Ausführungseinheit während des Zurücksetzens einen Störungszustand zu beheben, der sich aus einem spontanen Verarbeitungsfehler,
30 z. B. auf Grund von Informationsverlust durch den Einfluss von kosmischer oder sonstiger ionisierender Strahlung oder dergleichen ergeben kann. Strukturelle Mängel des Datenverarbeitungssystems von

- 2 -

schaltungstechnischer oder programmtechnischer Art,
die zu reproduzierbaren Fehlern in der Verarbeitung
führen, können von einem solchen „Watchdog“ nicht
abgefangen werden, da dieser das Auftreten der in
5 vorhersagbarer Weise zu dem Fehler führenden Bedin-
gungen nicht verhindern kann.

Eine weitere mögliche Ursache für Verarbeitungsfeh-
ler in einem elektronischen Datenverarbeitungssys-
10 tem sind Laufzeiteffekte. Da sich die elektrischen
Signale auf einem Halbleiterchip oder zwischen meh-
reren Chips eines Datenverarbeitungssystems nur mit
einer bestimmten Geschwindigkeit ausbreiten können,
müssen die Längen der Signalwege um so geringer und
15 um so genauer aufeinander abgestimmt sein, je höher
die Taktfrequenz ist, bei der das System betrieben
wird. Parasitäre Kapazitäten an den Signalleitungen
können Änderungen der Signalpegel verzögern. Da
diese parasitären Kapazitäten fertigungsbedingt
20 streuen können, ist es üblich, bei der Produktion
eines Prozessors zu testen, wie hoch die maximale
Taktfrequenz ist, bei der der Prozessor sicher ar-
beitet. Für diese Frequenz (abzüglich eines Sicher-
heitsabstands) wird der Prozessor freigegeben, und
25 es wird davon ausgegangen, dass er bei dieser frei-
gegebenen maximalen Frequenz und darunter liegenden
Taktfrequenzen sicher betrieben werden kann.

Es ist bereits vorgeschlagen worden, Prozessoren
30 für netzunabhängige Anwendungen je nach Auslas-
tungsgrad bei unterschiedlichen Taktfrequenzen zu
betreiben. Ziel dieser Maßnahme ist eine Minimie-
rung der Leistungsaufnahme des Prozessors. Da diese
linear mit der Taktfrequenz zunimmt, ist es an sich

wünschenswert, den Prozessor bei einer Taktrate zu betreiben, die nicht höher ist, als zur Bewältigung der aktuellen Aufgaben des Prozessors erforderlich.

5 Man kann feststellen, dass Alterungserscheinungen von elektronischen Bauelementen zu einer Zunahme der Wahrscheinlichkeit von spontanen Verarbeitungsfehlern in einem Datenverarbeitungssystem führen. Diese Steigerung kann zum Beispiel erklärt werden
10 durch langfristige Veränderungen an Grenzflächen der Halbleitersubstrate, auf denen die Schaltungen implementiert sind, und die zu Veränderungen der parasitären Kapazitäten führen, welche die Schaltungen belasten. Auch eine Migration von Dotierma-
15 terial in Schaltungselementen kann bei hohen Betriebstemperaturen nicht ausgeschlossen werden, wobei die Wirkungen einer solchen Migration um so stärker sind, je kleiner die auf den Halbleitersubstraten gebildeten Strukturen sind. In Anbetracht
20 der Entwicklung zu immer höheren Integrationsdichten ist daher mit einer zunehmenden Bedeutung von alterungsbedingten Zuverlässigkeitsproblemen zu rechnen.

25 Vorteile der Erfindung

Durch die vorliegende Erfindung, wie in Anspruch 1 definiert, wird ein Datenverarbeitungssystem geschaffen, welches trotz der oben geschilderten
30 Probleme langfristig ein hohes Maß an Betriebssicherheit garantiert und dadurch insbesondere für sicherheitskritische Anwendungen gut geeignet ist, bei denen es wichtig ist, spontane Funktionsausfälle soweit wie möglich zu vermeiden.

- 4 -

Diese Vorteile werden bei einem Datenverarbeitungssystem mit einer getaktet arbeitenden Ausführungseinheit, einem Taktgenerator zum Liefern eines Taktsignals für die Ausführungseinheit und einer Überwachungseinheit zum Überwachen des ordnungsgemäßen Arbeitens der Ausführungseinheit dadurch erreicht, dass der Taktgenerator eingerichtet ist, das Taktsignal mit einer steuerbaren Frequenz zu liefern und dass die Überwachungseinheit funktionsmäßig mit dem Taktgenerator verbunden ist, um die Frequenz des Taktsignals herabzusetzen, wenn nichtordnungsgemäßes Arbeiten der Ausführungseinheit festgestellt wird.

Es wird davon ausgegangen, dass die oben erläuterten parasitären Kapazitäten oder die eventuell durch Dotierungsmigration verursachte Verringerung der Effizienz von Schaltungsbauteilen für einen wesentlichen Teil von im Datenverarbeitungssystem auftretenden spontanen Fehlern verantwortlich ist. Indem im Fall des Auftretens solcher Fehler die Taktrate herabgesetzt wird, wird lediglich ein Teil der Rechenkapazität, die das System unter optimalen Bedingungen erreichen könnte, preisgegeben, die allgemeine Zuverlässigkeit des Systems bleibt jedoch erhalten.

Um im Falle einer Reduzierung der Taktrate eine auf dem Datenverarbeitungssystem laufende Nutzanwendung, die wenigstens zeitweise die mit einer ursprünglich spezifizierten hohen Taktrate erzielbare Rechenleistung des Systems voll ausschöpft, lauffähig zu erhalten, sollte die Nutzanwendung zweckmä-

- 5 -

ßigerweise in eine Mehrzahl von Funktionen gegliedert sein, wobei die Ausführung wenigstens einer der Funktionen, die als im Notfall verzichtbar beurteilt wird, in Abhängigkeit von der aktuellen
5 Taktrate des Systems zur Ausführung freigegeben oder nicht freigegeben ist.

Die Überwachungseinheit kann eine an sich bekannte Watchdog-Einheit umfassen, die nichtordnungsgemäßes
10 Arbeiten der Ausführungseinheit feststellt, wenn ein Funktionssignal von der Ausführungseinheit in einer vorgegebenen Zeitspanne ausbleibt, die aber im Falle des Ausbleibens nicht in herkömmlicher Weise das Datenverarbeitungssystem zurücksetzt,
15 sondern lediglich die Herabsetzung der Frequenz des Taktsignals veranlasst.

Alternativ oder in Kombination kann die Überwachungseinheit eingerichtet sein, eine Testverarbeitung durch die Verarbeitungseinheit bei einer aktuellen Taktrate und einer gegenüber der aktuellen
20 Taktrate veränderten Taktrate ausführen zu lassen und nichtordnungsgemäßes Arbeiten der Ausführungseinheit festzustellen, wenn das Ergebnis der bei
25 der aktuellen Taktrate durchgeführten Testverarbeitung und das Ergebnis der bei der veränderten Taktrate durchgeführten Testverarbeitung sich unterscheiden.

30 Vorzugsweise handelt es sich bei der veränderten Taktrate um eine gegenüber der aktuellen Taktrate erhöhte Taktrate. Dies erlaubt es, eine Neigung des Datenverarbeitungssystems, spontane Fehler zu produzieren, festzustellen, noch bevor die Grenz-

- 6 -

Taktfrequenz, oberhalb derer Verarbeitungsfehler auftreten, auf das Niveau der aktuellen Taktfrequenz abgesunken ist.

- 5 Die Überwachungseinheit, die die Ausführung der Testverarbeitung steuert, kann einfach und preiswert auf programmtechnischem Wege in der Ausführungseinheit implementiert sein.
- 10 Einer anderen Ausgestaltung zufolge umfasst die Überwachungseinheit eine zweite Ausführungseinheit und Mittel zum Vergleichen der Verarbeitungsergebnisse der zwei Ausführungseinheiten und ist eingerichtet, nichtordnungsgemäßes Arbeiten bei Nicht-
- 15 übereinstimmung der Ergebnisse festzustellen. Hier genügt eine einmalige Ausführung der Testverarbeitung, um die Zuverlässigkeit des Datenverarbeitungssystems zu beurteilen.
- 20 Auch bei dieser Ausgestaltung ist es zweckmäßig, für eine Prüfung der Betriebssicherheit die Taktfrequenz zeitweilig über eine aktuelle Taktfrequenz zu erhöhen und bei Feststellung von nicht ordnungsgemäßem Arbeiten bei der erhöhten Taktfrequenz die
- 25 Taktfrequenz unter besagte aktuelle Taktfrequenz abzusenken.

Das Datenverarbeitungssystem sollte über Mittel zum Ausgeben eines Warnsignals bei Absenkung der Taktfrequenz unter eine untere Grenze verfügen.

30

Insbesondere kann es sich bei dem Datenverarbeitungssystem um ein Steuergerät für ein Kraftfahrzeug, insbesondere ein Motorsteuergerät handeln.

Gegenstand der Erfindung ist auch ein Verfahren zum Betreiben einer getaktet arbeitenden Ausführungseinheit eines Datenverarbeitungssystems, insbesondere eines Datenverarbeitungssystems der oben beschriebenen Art, bei dem die Ausführungseinheit auf ordnungsgemäßes Arbeiten bei einer hohen Taktfrequenz geprüft wird und die Taktrate gesenkt wird, wenn nichtordnungsgemäßes Arbeiten der Ausführungseinheit festgestellt wird, wobei die Prüfung regelmäßig wiederholt wird. Die regelmäßige Prüfung kann insbesondere jeweils beim Ein- und/oder Ausschalten des Datenverarbeitungssystems oder periodisch während des Betriebs des Datenverarbeitungssystems vorgenommen werden.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung von Ausführungsbeispielen unter Bezugnahme auf die beigefügten Figuren.

Figuren

Fig. 1 ist ein Blockdiagramm eines Datenverarbeitungssystems gemäß einer ersten Ausgestaltung der Erfindung;

Fig. 2 ist ein Flussdiagramm eines von dem Datenverarbeitungssystem der Fig. 1 ausgeführten Betriebsverfahrens; und

Fig. 3 ist ein Blockdiagramm einer zweiten Ausgestaltung eines Datenverarbeitungssystems gemäß der Erfindung.

Beschreibung der Ausführungsbeispiele

Das in Fig. 1 schematisch dargestellte Datenverar-
5 beitungssystem umfasst einen Mikroprozessor 1, ei-
nen Arbeitsspeicher 2 und eine Überwachungseinheit
3, die über einen Daten- und Adressbus 4 miteinan-
der sowie gegebenenfalls mit nicht gezeigten Peri-
10 pherieeinheiten kommunizieren, die je nach Anwen-
dung des Systems unterschiedlich sein können und
zum Beispiel im Falle einer Anwendung als Mo-
torsteuergerät diverse Sensoren zum Erfassen von
Betriebsparametern des Motors und Aktoren zum Be-
einflussen dieser oder anderer Parameter des Motors
15 umfassen können. Das System umfasst ferner einen
Taktgenerator 5, der ein Taktsignal mit einer von
der Überwachungseinheit 3 über eine Steuerleitung 6
spezifizierten Frequenz über eine Taktleitung 7 an
den Mikroprozessor 1, den Arbeitsspeicher 2 und die
20 Überwachungseinheit 3 liefert.

Der Arbeitsspeicher 2 enthält Programmanweisungen
einer von dem Mikroprozessor 1 auszuführenden Nutz-
anwendung sowie einer Testverarbeitung.

25

Der Mikroprozessor 1 ist vom Hersteller für eine
Arbeits- Taktfrequenz spezifiziert. Unter normalen
Betriebsbedingungen steuert die Überwachungseinheit
3 den Taktgenerator 5 an, um diese spezifizierte
30 Taktfrequenz zu erzeugen, während der Mikroprozes-
sor 1 die Nutzenanwendung ausführt. Immer wenn das
System eingeschaltet wird, im Falle eines als Mo-
torsteuergerät arbeitenden Systems z. B. durch Dre-
hen eines Zündschlüssels, führt der Mikroprozessor

1 vor Beginn der Nutzanwendung eine Initialisierung
aus, deren Ablauf anhand von Fig. 2 erläutert wird.
In einem ersten Schritt S1 setzt die Überwachungs-
einheit 3 die Taktfrequenz f des Taktgenerators auf
5 die für den Mikroprozessor 1 spezifizierte Frequenz
 f_{nom} . Bei dieser Taktfrequenz führt der Mikroprozes-
sor 1 in Schritt S2 die bereits erwähnte Testverar-
beitung aus. Diese Testverarbeitung kann z. B. aus
einer Folge von arithmetischen oder logischen Ope-
10 rationen bestehen, die an aus dem Arbeitsspeicher 2
gelesenen Konstanten durchgeführt werden und daher
bei jeder Durchführung das gleiche Endergebnis lie-
fern sollten. Der letzte Schritt S3 der Testverar-
beitung ist ein Schreiben des Ergebnisses an eine
15 Adresse, die der Überwachungseinheit 3 zugeordnet
ist, so dass diese das Ergebnis R_{nom} empfängt und
zwischenspeichert.

Anschließend erhöht die Überwachungseinheit 3 die
20 Taktfrequenz f auf $f_{nom} + \Delta$ (S4) und lässt den Mikro-
prozessor 1 die Testverarbeitung bei dieser erhöh-
ten Taktfrequenz wiederholen (S5). Das Ergebnis R_{inc}
wird auf diese Weise wiederum in die Überwachungs-
einheit 3 geschrieben (S6). Diese vergleicht nun in
25 Schritt S7 die zwei empfangenen Ergebnisse R_{nom} und
 R_{inc} . Bei Übereinstimmung wird davon ausgegangen,
dass der Prozessor 1 bei beiden Taktfrequenzen, f_{nom}
und $f_{nom} + \Delta$, korrekt gearbeitet hat. In diesem Fall
wird in Schritt S8 die Taktfrequenz f auf f_{nom} zu-
30 rückgesetzt, und der Mikroprozessor 1 beginnt, die
Nutzanwendung auszuführen.

Falls in Schritt S7 Nichtübereinstimmung der Ergeb-
nisse festgestellt wird, so bedeutet dies, dass die

- 10 -

- erhöhte Taktfrequenz $f_{\text{nom}} + \Delta$ nicht betriebssicher ist. Um von dieser nichtbetriebssicheren Frequenz einen Sicherheitsabstand einzuhalten, wird in Schritt S9 eine neue, verringerte Betriebsfrequenz
- 5 $f = f_{\text{nom}} - \Delta$ eingestellt. In Schritt S10 überprüft der Mikroprozessor 1 anhand einer vom Hersteller des Systems vorbereiteten und im Arbeitsspeicher 2 abgelegten Liste, ob die Nutzanwendung Funktionen enthält, deren Ausführung bei der reduzierten Taktrate
- 10 gesperrt werden muss, um die Funktionsfähigkeit der Nutzanwendung in ihren wesentlichen Merkmalen aufrecht zu erhalten und unzulässig lange Reaktionszeiten der Nutzanwendung auf äußere Ereignisse zu verhindern und diese Funktionen gegebenenfalls zu
- 15 sperren. Des weiteren wird in Schritt S10 eine Warnanzeige an einen Benutzer ausgegeben, wenn wenigstens eine der folgenden Bedingungen erfüllt ist:
- 20 a) eine abermalige Verringerung der Taktfrequenz um Δ würde die Sperrung wenigstens einer Funktion der Nutzanwendung erforderlich machen;
- b) die Verringerung der Taktrate in Schritt S9
- 25 hat zur Sperrung einer Funktion geführt;
- c) es sind bereits alle für die Nutzanwendung nicht lebenswichtigen Funktionen gesperrt, so dass eine weitere Verringerung der Taktrate nicht durch
- 30 Sperrung weiterer Funktionen aufgefangen werden könnte, sondern zur Inoperabilität des gesamten Systems führen würde.

Die Schritte S1 bis S3 einerseits und S4 bis S10 andererseits müssen nicht unbedingt zeitlich aufeinanderfolgend ausgeführt werden. So ist es z. B. denkbar, die Schritte S1 bis S3 nur einmal während
5 einer erstmaligen Inbetriebnahme des Systems durchzuführen und ihr Ergebnis R_{nom} in der Überwachungseinheit 3 gespeichert zu halten, so dass spätere Prüfungen der Betriebssicherheit des Systems sich auf die Durchführung S4 bis S10 beschränken können.

10 Dies ist insbesondere dann zweckmäßig, wenn Überprüfungen der Betriebssicherheit auch periodisch bei laufendem System durchgeführt werden, da zum Durchführen der Schritte S4 bis S10 die Nutzenanwendung nur etwa halb so lang unterbrochen werden muss
15 wie für die Durchführung des gesamten in Fig. 2 gezeigten Verfahrens.

Um den Start der Nutzenanwendung nicht durch die Betriebssicherheitsprüfung gemäß Fig. 2 zu verzögern, kann auch vorgesehen werden, dass diese Prüfung nicht jeweils bei Inbetriebnahme des Systems, sondern unmittelbar vor dessen Ausschalten durchgeführt wird, wobei natürlich in diesem genau wie im
20 vorhergehenden Fall eine eventuell in Schritt S9 neu festgelegte Betriebsfrequenz f bei einer anschließenden Wiederholung des Verfahrens als die spezifizierte Frequenz f_{nom} verwendet wird.

30 Zusätzlich zu der oben beschriebenen Aufgabe des Vergleichens der Ergebnisse R_{nom} und R_{inc} der zwei Testverarbeitungen kann die Überwachungseinheit 3 in an sich bekannter Weise auch noch die Aufgabe des Erfassens eines undefinierten Betriebszustandes

oder Absturzes des Mikroprozessors 1 wahrnehmen. Zu diesem Zweck ist die Nutzenanwendung so ausgelegt, so dass sie in regelmäßigen Zeitabständen die Erzeugung eines Totmannsignales veranlasst, welches von
5 der Überwachungseinheit 3 empfangen wird. Dieses Totmannsignal kann z. B. ein Lesezugriff auf die oben erwähnte Adresse sein, an welche der Mikroprozessor 1 die Ergebnisse der Testverarbeitung schreibt. Dieses Totmannsignal setzt in der Überwachungseinheit 3 jeweils einen Zeitgeber zurück,
10 dessen Latenzzeit länger als der vorgesehene Zeitabstand zwischen zwei Totmannsignalen ist. Solange die Totmannsignale im vorgesehenen Zeitabstand eintreffen, wird der Zeitgeber regelmäßig zurückgesetzt und kann nicht ablaufen. Wenn im Folge eines
15 Prozessorabsturzes das Totmannsignal ausbleibt und der Zeitgeber abläuft, löst die Überwachungseinheit 3 über eine Resetleitung 8 (Fig. 1) einen Reset des Mikroprozessors 1 aus und veranlasst diesen so, die
20 Nutzenanwendung neu zu starten.

Fig. 3 zeigt eine zweite Ausgestaltung eines erfindungsgemäßen Datenverarbeitungssystems mit zwei Mikroprozessoren 1, 11, die jeweils über einen Daten-/Adressbus 4, 14 mit einem zugeordneten Arbeitsspeicher 2, 12 und gegebenenfalls mit nicht
25 dargestellten Peripherieeinheiten kommunizieren. Ein Datenverarbeitungssystem mit einer solchen Struktur kommt insbesondere bei einem Motorsteuergerät für einen Motor mit sechs oder mehr Zylindern in Betracht, bei welchem die Zylinder in zwei Gruppen aufgeteilt sind, welche jeweils von einem der
30 zwei Prozessoren 1, 11 gesteuert werden. Die Prozessoren 1, 11 empfangen ein Taktsignal von einem

- 13 -

gemeinsamen Taktgenerator 5 über eine Taktleitung 7. Die Frequenz des Taktsignals ist gesteuert durch eine ebenfalls beiden Prozessoren 1, 11 gemeinsam zugeordnete Überwachungseinheit 3. Alle Adern der Busse 4, 14, sowohl Daten- als auch Adressleitungen, liegen an einer Bank von XOR-Gattern 20 an, deren Ausgang jeweils genau dann den Wert „wahr“ annimmt, wenn sich die Werte auf den zwei homologen Adern der Busse 4, 14, die an den zwei Eingängen eines gleichen Gatters 20 anliegen, unterscheiden. Die Ausgänge der XOR-Gatter 20 sind jeweils mit einem Eingang eines OR-Gatters 21 verbunden, dessen Ausgang folglich immer dann den Wert „wahr“ annimmt, wenn sich die Werte auf zwei beliebigen homologen Adern der Busse 4, 14 unterscheiden.

Resetleitungen 8, die die gleiche Funktion wie bei der Ausgestaltung der Fig. 1 erfüllen, können zwischen der Überwachungseinheit 3 und den Prozessoren 1, 11 vorgesehen sein.

Mögliche Arbeitsweisen dieser Ausgestaltung werden im Folgenden ebenfalls unter Rückgriff auf Fig. 2 beschrieben.

Einer ersten Alternative zufolge beginnt die Überwachungseinheit 3 die Betriebssicherheitsprüfung, indem sie wie in Schritt S4 die Frequenz des Taktsignals f über eine aktuell im Normalbetrieb verwendete Frequenz f_{nom} hinaus erhöht und dann eine Testverarbeitung (S5) durch die Mikroprozessoren 1, 11 ausführen lässt, deren Ergebnisse von der Nutzanwendung nicht benötigt werden, sondern die lediglich der Sicherheitsprüfung dient. Während dieser

- 14 -

Verarbeitung vergleichen die Logikgatter 20, 21 fortlaufend die von den Mikroprozessoren 1, 11 erzeugten Daten und Adressen, entsprechend dem Schritt S7 der Fig. 2. Wenn diese Daten und Adressen während der gesamten Testverarbeitung gleich sind, arbeiten beide Prozessoren 1, 11 sicher, und die Taktfrequenz wird in Schritt S8 auf f_{nom} zurückgesetzt. Falls jedoch eine Abweichung in einem Datenwert oder einer Adresse auftritt, verzweigt das Verfahren zu Schritt S9, wo die Taktfrequenz herabgesetzt wird, und in Schritt S10 wird, wie bereits oben erläutert, festgelegt, ob und gegebenenfalls welche Funktionen des Anwendungsprogramms gesperrt werden müssen, und gegebenenfalls eine Warnung an den Benutzer ausgegeben.

Da gemäß dieser Ausgestaltung nicht nur Endergebnisse der Testverarbeitung verglichen werden, sondern auch sämtliche Zwischenergebnisse einschließlich der angesprochenen Adressen, wird bei gleicher Anzahl von Programmschritten der Testverarbeitung ein Fehler mit höherer Wahrscheinlichkeit als bei der ersten Ausgestaltung erfasst.

Zusätzlich bietet das Datenverarbeitungssystem der Fig. 3 die Möglichkeit, Fehler der Prozessoren 1, 11 auch dann zu erfassen, wenn diese gleichzeitig identische Anweisungen bei der normalen Taktfrequenz f_{nom} ausführen, z. B. in einer Startphase der Nutzanwendung, in welcher für beide Prozessoren 1, 11 identische Initialisierungen vorgenommen werden. Dies erlaubt eine Prüfung der Betriebssicherheit völlig ohne Zeitaufwand.

- 15 -

Prozessoren und Überwachungseinheiten sind in den obigen Beispielen als getrennte Einheiten beschrieben worden. Selbstverständlich können aber auch Prozessoren mit einer in die Prozessorschaltungen integrierten, fest verdrahteten Fehlererkennungsfunktion zum Erkennen von ECC- oder Paritätsfehlern in durch den Prozessor gelesenen Daten zum Einsatz kommen; ein solcher Prozessor kann als Kombination von Prozessor und Überwachungseinheit im Sinne der vorhergehenden Beschreibung aufgefasst werden.

Patentansprüche

- 5
1. Datenverarbeitungssystem mit einer getaktet arbeitenden Ausführungseinheit (1), einem Taktgenerator (5) zum Liefern eines Taktsignals für die Ausführungseinheit (1) und
- 10 einer Überwachungseinheit (3) zum Überwachen des ordnungsgemäßen Arbeitens der Ausführungseinheit (1), dadurch gekennzeichnet, dass der Taktgenerator (5) eingerichtet ist, das Taktsignal mit einer steuerbaren Frequenz zu liefern und dass die Überwachungseinheit (3) funktionsmäßig mit dem Taktgenerator (5) verbunden ist, um die Frequenz des Taktsignals herabzusetzen, wenn nichtordnungsgemäßes Arbeiten der Ausführungseinheit (1) festgestellt wird.
- 15
- 20
2. Datenverarbeitungssystem nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungseinheit (3) eine Watchdog-Einheit umfasst, die nichtordnungsgemäßes Arbeiten der Ausführungseinheit feststellt, wenn ein Funktionssignal von der Ausführungseinheit in einer vorgegebenen Zeitspanne ausbleibt.
- 25
- 30 3. Datenverarbeitungssystem nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungseinheit (3) eingerichtet ist, eine Testverarbeitung von der Verarbeitungseinheit bei einer aktuellen Taktrate (f_{nom}) und

- 17 -

- einer gegenüber der aktuellen Taktrate veränderten Taktrate ausführen zu lassen und nichtordnungsgemäßes Arbeiten der Ausführungseinheit festzustellen, wenn das Ergebnis der bei der aktuellen Taktrate durchgeführten Testverarbeitung und das Ergebnis der bei der veränderten Taktrate durchgeführten Testverarbeitung sich unterscheiden.
4. Datenverarbeitungssystem nach Anspruch 3, dadurch gekennzeichnet, dass die veränderte Taktrate ($f_{\text{nom}} + \Delta$) eine gegenüber der aktuellen Taktrate (f_{nom}) erhöhte Taktrate ist.
5. Datenverarbeitungssystem nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass die Überwachungseinheit (3) programmtechnisch in der Ausführungseinheit (1) implementiert ist.
6. Datenverarbeitungssystem nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungseinheit (3, 11, 20, 21) eine zweite Ausführungseinheit (11) und Mittel (20, 21) zum Vergleichen der Verarbeitungsergebnisse der zwei Ausführungseinheiten (1, 11) umfasst und eingerichtet ist, nichtordnungsgemäßes Arbeiten bei Nichtübereinstimmung der Ergebnisse festzustellen.
7. Datenverarbeitungssystem nach Anspruch 6, dadurch gekennzeichnet, dass der Taktgenerator (5) eingerichtet ist, die Taktrate

- 18 -

- 5 zeitweilig über eine aktuelle Taktrate zu
erhöhen (S4) und bei Feststellung von
nichtordnungsgemäßem Arbeiten bei der er-
höhten Taktrate die Taktrate unter besagte
aktuelle Taktrate abzusenken (S9).
8. Datenverarbeitungssystem nach einem der
vorhergehenden Ansprüche, dadurch gekenn-
zeichnet, dass sie Mittel zum Ausgeben ei-
10 nes Warnsignals bei Absenkung der Taktrate
unter eine untere Grenze verfügt.
9. Datenverarbeitungssystem nach einem der
vorhergehenden Ansprüche, dadurch gekenn-
15 zeichnet, dass die Ausführungseinheit (1)
ferner eingerichtet ist, eine Nutzenanwendung
auszuführen, die eine Mehrzahl von Funktio-
nen umfasst, wobei die Ausführung wenigstens
einer der Funktionen in Abhängigkeit
20 von der aktuellen Taktrate des Systems
freigegeben oder nicht freigegeben ist.
10. Datenverarbeitungssystem nach einem der
vorhergehenden Ansprüche, dadurch gekenn-
25 zeichnet, dass es ein Kfz-Steuergerät ist.
11. Verfahren zum Betreiben einer getaktet ar-
beitenden Ausführungseinheit (1) eines Da-
tenverarbeitungssystems, insbesondere nach
30 einem der vorhergehenden Ansprüche, bei dem
die Ausführungseinheit (1) auf ordnungs-
gemäßes Arbeiten bei einer hohen Taktrate ge-
prüft (S4-S7) und die Taktrate gesenkt wird
(S9), wenn nichtordnungsgemäßes Arbeiten

- 19 -

der Ausführungseinheit festgestellt wird, dadurch gekennzeichnet, dass die Prüfung regelmäßig wiederholt wird.

- 5 12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Prüfung jeweils beim Ein- und/oder Ausschalten des Datenverarbeitungssystems vorgenommen wird.
- 10 13. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Prüfung periodisch während des Betriebs des Datenverarbeitungssystems vorgenommen wird.

1/2

Fig. 1

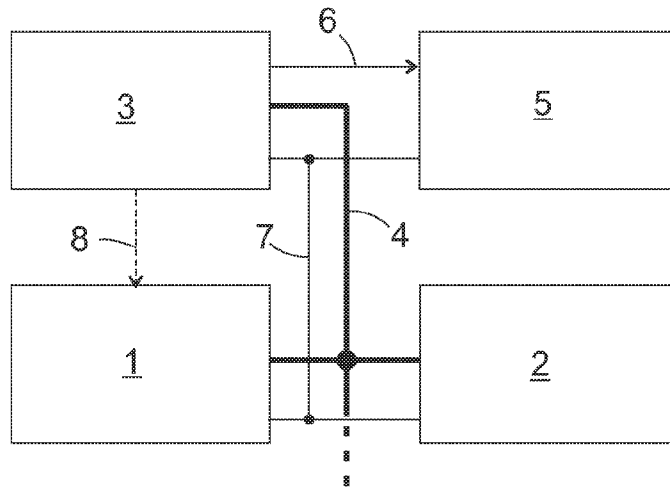


Fig. 2

